JACKIE SPEIER
14TH DISTRICT, CALIFORNIA

2465 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515-0514
(202) 225-3531
FAX: (202) 226-4183

155 BOVET ROAD, SUITE 780
SAN MATEO, CA 94402
(650) 342-0300
FAX: (650) 375-8270

WWW.SPEIER.HOUSE.GOV
WWW.FACEBOOK.COM/JACKIESPEIER
WWW.TWITTER.COM/REPSPEIER

Congress of the United States
House of Representatives
Washington, DC 20515-0514

COMMITTEE ON ARMED SERVICES
SUBCOMMITTEES:
RANKING MEMBER, MILITARY PERSONNEL
EMERGING THREATS

PERMANENT SELECT COMMITTEE
ON INTELLIGENCE
SUBCOMMITTEES:
EMERGING THREATS
NSA AND CYBERSECURITY

Senior Whip

February 1, 2018

The Honorable James Mattis
Secretary of Defense
1000 Defense Pentagon
Washington, DC 20301

Dear Secretary Mattis:

We are writing in response to an article in the Washington Post on January 29, 2018, titled "U.S. soldiers are revealing sensitive and dangerous information by jogging.[1]" The article describes maps generated by GPS tracking company Strava that reveal sensitive locations and activities of individuals at U.S. military bases around the world. Subsequent information from a Pentagon spokesman indicates that the Defense Department Acting Chief Information Officer will lead a department-wide review to determine what policy changes may be needed.[2]

According to the article, users of the Strava maps allegedly acquired the locations of a Patriot missile site in Yemen, Special Operations bases in the Sahel, and a suspected base under construction in Syria, among other sites. Details shared from wearable technology used by personnel at these sites, even for locations that are overt and publicly known, create a vast amount of easily accessible data on individuals' identities, patterns of life, and operations. Such widely available data increases terrorism and counterintelligence threats to our personnel and facilities.

As members of the House Committee on Armed Services, we are concerned with the potential security risks that the use of wearable technology and smart devices could create to U.S. military personnel and facilities around the world. Given the large number of DoD facilities with varying levels of sensitivity, it seems plausible that policies on the use of these devices may be unevenly implemented. This operational security problem is not isolated to FitBits and other wearable devices, but also personal GPS, smart phones, smart cars, and other smart technology. We are also concerned that we find ways to keep personnel connected with their friends and family while accounting for operational security needs.

[1] https://www.washingtonpost.com/world/a-map-showing-the-users-of-fitness-devices-lets-the-world-see-where-us-soldiers-are-and-what-they-are-doing/2018/01/28/86915662-0441-11e8-aa61-f3391373867e_story.html?utm_term=.178cdab3b8d7

[2] https://www.washingtonpost.com/world/the-us-military-reviews-its-rules-as-new-details-of-us-soldiers-and-bases-emerge/2018/01/29/6310d518-050f-11e8-aa61-f3391373867e_story.html?hpid=hp_rhp-top-table-main_strava0130-1253pm%3Ahomepage%2Fstory&utm_term=.e6168a2d92cf

We respectfully request your Department provide an update on the review of security protocols relating to this issue, to include restrictions on the presence or use of smart technology. In particular, we request answers to the following questions:

- What is the timeline of the CIO review, its draft conclusions, and what policy changes are being considered and implemented?
- What is the Defense Department's current policy on use of "smart" technology that transmits user data at overseas bases? At classified overseas facilities? What processes does the Department have in place to periodically review such policies? Who is responsible for ensuring that these policies are implemented?
- What operational security training does the Department of Defense or individual military services require for individuals traveling or deploying overseas?
- What red cell testing has the Department of Defense conducted on this risk and what are the results of the tests?
- What safeguards does the Department have in place to prevent personnel user-generated data from being used by adversaries seeking to collect intelligence on and/or compromise individuals?
- What terrorist or foreign intelligence activity has been connected to the use of open source information, such as that generated by wearable devices?
- What are Department processes for mitigating security risks once a sensitive facility or program is publicly exposed? How is this information reported within the Department? How is this information reported to Congress?

Thank you for your attention to this matter, and for your prompt response within two weeks of your receipt of this letter.

Sincerely,

Jackie Speier

Jackie Speier
Member of Congress

Donald M. Payne, Jr.
Member of Congress

Debbie Dingell

Debbie Dingell
Member of Congress

Seth Moulton
Member of Congress

Walter B. Jones

Walter B. Jones
Member of Congress

Carol Shea-Porter

Carol Shea-Porter
Member of Congress

Ted W. Lieu

Ted W. Lieu
Member of Congress

James P. McGovern
Member of Congress

Jamie Raskin
Member of Congress

John Garamendi

John Garamendi
Member of Congress

Jim Cooper
Member of Congress